

REMARKS

The Office Action dated November 16, 2005 has been received and carefully noted. The above amendments to the specification and the following remarks are submitted as a full and complete response thereto.

The Abstract is amended to remove legal phraseology. No new matter is added. Claims 33-68 are respectfully submitted for consideration.

As a preliminary matter, Applicant respectfully disagrees with some allegations made in the "Response to Arguments" section of the Office Action.

First, the Office Action on page 2, alleged that the Response filed on August 16, 2005 did not comply with 37 C.F.R. 111(b), because the Response did not "specifically [point] out how the language of the claims patentably distinguishes them from the references." As will be repeated below, Applicant's response on page 7 clearly stated that "[i]t is respectfully submitted that, the cited combination of references fails to disclose or suggest at least the feature of 'defining a criteria for selecting a one of a plurality of different security methods', as recited in claims 33 and 63-68 of the present application." The reasons supporting this assertion are properly presented in pages 7 to 10 of the August 16, 2006 Response. Thus, the Response filed on August 16, 2005, as well as, the present Response, fully complies with 37 C.F.R. 111(b).

Next, the Office Action asserted that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of

references.” However, as a rebuttal to the Office Action’s allegations of where certain elements of the pending claims are disclosed in a particular reference, arguments traversing these allegations even if directed to the single reference, are appropriate. Further, the August 16, 2005 Response clearly states on page 10 “it is respectfully submitted that the cited combination of references taken either individually or in combination fails to disclose or suggest all of the features recited in claims 33 and 63-68.” (Underline added).

The Office Action objected to the specification because the Abstract contains legal phraseology. Applicant respectfully submits that the Abstract as amended does not contain legal phraseology. Accordingly, withdrawal of the objection to the specification is respectfully requested.

The Office Action rejected claims 33-42 and 58-68 under 35 U.S.C. 103(a) as being obvious over U. S. Patent No. 5,642,401 to Yahagi (Yahagi), in view of U.S. Patent No. 5,991,407 to Murto (Murto). The Office Action took the position that Yahagi discloses all of the features recited in the above-identified claims except the feature of a plurality of messages selected from a set of message types, and asserts that Murto discloses this feature. This rejection is respectfully traversed.

Claim 33, upon which claims 34-62 depend, recites a method of securing communication between a first party and a second party in a telecommunications network. The method includes the step of defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each including a

plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The method also includes the steps of selecting one of the plurality of different security methods in accordance with defined criteria and performing the security method.

Claim 63 recites a telecommunications network element for securing communication between a first party and a second party. The network element includes means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each including a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The network element also includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria and means for insuring that the communication between the first and second parties is in accordance with the selected security method.

Claim 64 recites a terminal for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The terminal further includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and means for ensuring that the communication between the first and second party is in accordance with the selected security method.

Claim 65 recites a system for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The system further includes a selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and a means for ensuring that the communication between the first and second party is in accordance with the selected security method.

Claim 66 recites a computer program product comprising computer-readable code, the computer-readable code causes a computer to perform a procedure for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The computer code further includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and a means for ensuring that the communication between said first and second party is in accordance with said selected security method.

Claim 67 recites a method of securing communication between a first party and a second party in a telecommunications network including the steps of defining a criteria for selecting one of a plurality of different security methods each having a different set of

steps for performing the respective security methods, the plurality of security method each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The method further includes selecting one of the plurality of different security methods in accordance with the defined criteria, and performing the security method.

Claim 68 recites a method of securing communication between a first party and a second party in a telecommunications network including the steps of defining a criteria for selecting one of a plurality of different security methods each having a different set of steps for performing the respective security methods, the plurality of security method each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common, selecting one of the plurality of different security methods in accordance with the defined criteria, and performing the security method.

According to embodiments of the present invention, the first party and second party may be a mobile station and a base station. The set of message types may include messages such as random number messages, hash function messages, signature function messages, parameters for use with function messages, security parameter messages, keys for function messages, encoded messages, messages to and/or from a third party and authentication response messages. These are all particular message types that may be used in authenticating a mobile station for use in a communication network. Thus, it is possible to select from a large number of different security methods. It is respectfully

submitted that the claimed invention advantageously allows a relatively large number of different security methods to be implemented using only a small number of different messages. As shown at least in Figures 3 – 9, the claimed invention includes a plurality of different security methods. Accordingly, independent claims 33 and 63-68 recite the feature of selecting a security method from a plurality of security methods.

Applicant respectfully submits that each of the pending claims recite features that are neither disclosed nor suggested in any of the cited references taken individually, or in combination.

Yahagi is directed to an authentication method whereby a base station authenticates a mobile station. The method include selecting a random number $RAND(j)$ and corresponding authentication calculations are made from a plurality of parameters $RAND(1...n)$ and $SRES(1...n)$ respectively (for example, see column 2 lines 1-13 of Yahagi). The method further includes a method key K_i that is specific to the mobile station being authenticated (for example, see column 4 lines 18-23 of Yahagi).

Murto is directed to an authentication method whereby each subscriber is allocated an IMSI (International Mobile Subscriber Identity) number, a subscriber authentication key K_i , a plurality of “triplets” (K_c , $RAND$, $SRES$) for use in authenticating that subscriber (for example, see column 1 lines 37-55 of Murto). Each value of $SRES$ and K_c is calculated based on K_i and a respective value of $RAND$ (for example, see column 1 lines 49-53 of Murto).

Applicant respectfully submits that the cited references, individually or combined, fail to disclose or suggest at least the feature of defining criteria for selecting one of a plurality of different security methods, as recited in claim 33 and similarly recited in claims 63-68.

Instead, Yahagi discloses an “authentication algorithm calculation means 6 [that] performs an authentication calculation by using an authentication random number sent from a base station 2 and the authentication key 5 as input parameters” (column 3, lines 63-67). In Figure 3 thereof, Yahagi further discloses the steps of a single authentication method. The single method merely selects a random number from a plurality of random numbers. Regardless of which random number is chosen, the same authentication method is used because the use of different random numbers merely changes the parameters of the single authentication method. The Office Action alleged that the values RAND(1...n) and SRES(1...n) of Yahagi can be interpreted as a plurality of method steps. However, Yahagi (col. 2 lines 7-24) merely discloses a single security method, which is a function of a random number. Therefore, the same method is used regardless of which of the parameters are utilized in the authentication method. Thus, any reasonable interpretation of Yahagi will have to show how a different method is used for authentication, regardless of the values of the random parameters, RAND.

As an analogy, please consider the scenario wherein a person selects one car from a plurality of cars to travel from one destination to another. Regardless of whether the person selects a blue car from a plurality of cars that are blue, green, brown or black, the

same method of travel is used. The choice of car, even if performed randomly, does not change the method of travel. On the other hand, a person who chooses a method of travel from a plurality of methods of travel, may select from a car, airplane or train.

The Office Action admits that Yahagi does not disclose the feature of a plurality of messages selected from a set of message types and alleges that Murto cures this deficiency.

Murto discloses an authentication procedure in a GSM-based mobile communications system. The Office Action relies on Murto to disclose the feature of a plurality of messages selected from a set of message types. Murto, similar to Yahagi, discloses a GSM authentication method involving selecting a random number RAND from a plurality of random numbers $RAND(1...n)$ and calculating a respective authentication result SRES. As discussed above, the method of Murto includes selecting one of a plurality of “triplets” each comprising a random number RAND, an authentication result SRES and a ciphering key K_c (see column 5 lines 35-45 of Murto). These triplets are derived using pairs of values IMSI and K_i , (alleged plurality of message types).

Therefore, the cited references taken individually or in combination, fail to disclose or suggest all of the features recited in any of the pending claims.

Applicant respectfully submits that because claims 34-42 and 58-62 depend from claim 33, these claims are allowable at least for the same reasons as claim 33, as well as the additional features recited in these dependent claims.

Based at least on the above, Applicant respectfully submits that the cited references taken individually or in combination, fail to disclose or suggest all of the features recited in claims 33-42 and 58-68. Accordingly, withdrawal of the rejection of claims 33-42 and 58-68 under 35 U.S.C. 103(a) is respectfully requested.


Applicant gratefully acknowledges the indication that claims 43-57 would be allowable if rewritten in independent form. However, Applicant submits that these claims are allowable in their present form at least for the same reasons as claim 33. Accordingly, withdrawal of the objection to claims 43-57 is respectfully requested.

Applicant respectfully submits that, at least in view of the above, each of claims 33-68 of the present application contain allowable subject matter. Therefore it is respectfully requested that all claims pending in the present application be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,


David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DEB:jkm

Enclosures: Petition for Extension of Time
Check No. 14436